

Formation Sécuriser son infrastructure dans AWS

■ Durée :	3 jours (21 heures)
■ Tarifs inter-entreprise :	2 475,00 € HT (standard) 1 980,00 € HT (remisé)
■ Public :	Architectes et administrateurs AWS, ingénieurs systèmes / réseaux, équipes Cloud, RSSI techniques
■ Pré-requis :	Expérience de base sur AWS (console, services principaux EC2, S3, RDS, VPC) et en sécurité des SI
■ Objectifs :	Comprendre l'architecture AWS et les briques principales sous l'angle de la sécurité - Mettre en œuvre les bonnes pratiques de sécurisation des comptes, identités, réseaux, données et services AWS - Utiliser les services natifs (Security Hub, GuardDuty, IAM, KMS, CloudTrail, Config...) pour contrôler et auditer la sécurité - Concevoir une architecture AWS durcie adaptée à son contexte
■ Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
■ Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
■ Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
■ Référence :	CYB102775-F

■ Note de satisfaction des participants:	Pas de données disponibles
■ Contacts :	commercial@dawan.fr - 09 72 37 73 73
■ Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
■ Délais d'accès :	Variable selon le type de financement.
■ Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre l'architecture AWS et la responsabilité partagée

Revoir l'organisation AWS : comptes, organisations, régions, availability zones

Analyser le modèle de responsabilité partagée d'AWS

Identifier les services fondamentaux à sécuriser (EC2, S3, RDS, IAM, VPC, etc.)

Découvrir les services de sécurité natifs : Security Hub, GuardDuty, Config, Inspector

Atelier fil rouge : dresser la carte des services AWS utilisés dans un cas d'école et identifier les points critiques

Sécuriser identités, accès et comptes AWS

Mettre en œuvre IAM : utilisateurs, rôles, groupes, politiques

Appliquer le moindre privilège et segmenter les responsabilités (rôles applicatifs, admins, comptes de service)

Sécuriser l'accès aux comptes : MFA, AWS SSO / IAM Identity Center, politiques de mot de passe

Auditer l'utilisation des identités et détecter les clés d'accès à risque

Atelier fil rouge : concevoir une structure IAM pour une application multi-environnements (dev, test, prod)

Sécuriser le réseau et les services exposés

Concevoir des VPC sécurisés : sous-réseaux publics / privés, tables de routage, NAT, endpoints VPC

Configurer les Security Groups et Network ACLs pour contrôler les flux

Protéger les applications exposées avec AWS WAF, CloudFront, ALB / NLB

Gérer les accès distants (bastions, Session Manager) et limiter les accès administratifs

Atelier fil rouge : proposer une architecture VPC sécurisée pour une application web en production

Protéger les données et les services managés AWS

Sécuriser les buckets S3 (politiques de bucket, block public access, chiffrement, logs d'accès)

Protéger les bases de données RDS et autres services managés (Aurora, DynamoDB, etc.)

Utiliser KMS pour la gestion des clés de chiffrement et le chiffrement des données au repos

Mettre en place des sauvegardes et des plans de reprise pour les services critiques

Atelier fil rouge : auditer une configuration S3 / RDS et proposer des mesures de durcissement simples et rapides

Superviser la sécurité AWS et améliorer la posture en continu

Activer et exploiter CloudTrail, CloudWatch Logs et AWS Config pour la traçabilité et la conformité

Utiliser Security Hub, GuardDuty et Inspector pour détecter anomalies, menaces et vulnérabilités

Construire des tableaux de bord sécurité ciblés pour les équipes techniques et la direction

Mettre en place une démarche d'amélioration continue de la sécurité AWS

Atelier fil rouge final : définir un plan d'actions priorisé à partir des alertes GuardDuty et des findings Security Hub